STATEWIDE INFORMATION SYSTEMS POLICY

Statewide Policy: Usernames and Passwords

Product ID: ENT-SEC-063

Effective Date: June 2005

Approved: Janet R. Kelly, Director, Department of Administration

Replaces & Supercedes: This policy supercedes any prior enterprise policies for establishing and implementing information technology (IT) policies and standards.

I. Authorizations, Roles, & Responsibilities

Pursuant to the Montana Information Technology Act ("MITA") (Title 2, Chapter 17, Part 5 of the Montana Code Annotated ("MCA"), it is the policy of the state that information technology be used to improve the quality of life of Montana citizens, and that such improvement is to be realized by protecting individual privacy and the privacy of the information contained within the state's information technology systems. §2-17-505(1), MCA. It is also the policy of the state that the development of information technology resources be conducted in an organized, deliberative, and cost-effective manner, which necessitates the development of statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and others using the state network. It is also anticipated that State information technology systems will be developed in cooperation with the federal government and local governments with the objective of providing seamless access to information and services to the greatest degree possible. §2-17-505(2), MCA.

Department of Administration: Under MITA, the Department of Administration ("DOA") is responsible for carrying out the planning and program responsibilities for information technology for state government (except the national guard), including for establishing and enforcing a state strategic information technology plan and establishing and enforcing statewide information technology policies and standards. DOA is responsible for implementing MITA and all other laws for the use of information technology in state government. The director of DOA has appointed the chief information officer to assist in carrying out the department's information technology duties. §2-17-512, MCA.

Department Heads: Each department head is responsible for ensuring an adequate level of security for all data within their department. §2-15-114, MCA.

II. Policy - Requirements

A. Scope

This policy must be followed for any systems requiring a password. It is the user's responsibility to follow the requirements of this policy for any password.

B. Purpose

This policy outlines the procedures for the use of usernames and passwords to control unauthorized use of the network, to prevent the intentional or unintentional modification, destruction, disclosure, or misuse of data and information resources for which the State of Montana is responsible.

All agencies are responsible for authorizing access to their information resources by designating certain persons as users and authorizing such persons to access these resources in the manner necessary for performing their duties.

1. Key Definitions

For the purposes of this policy, the following definitions apply:

User: An individual with access to a computer system or network.

Login: The process of authenticating a user into a computer system or network. Typically this consists of a two-part process in which the user supplies a username and a password.

Username : A set of characters used as a unique identifier for an individual when authenticating to a computer system or network.

Password: A set of characters used to establish an individual's authenticated access to a computer system or network. The password is a correlated piece of information that is used with the username to ensure that the username being entered is being entered by the correct individual.

External User: The term external user is used as a term for those users needing access to public state eGovernment services for non-state employee purposes. This could be for personal or business related activities not associated with a state job function.

Internal User: The term internal user is used to describe a state employee, contractor, or other user doing business for the state that needs access to state systems to perform his or her job functions.

2. External User – Usernames

A user must be identified to the network with a unique username. Each username must have a minimum of 6 characters and must have a password associated with it.

A username is to be deactivated when the individual user no longer needs access to a computer system.

Usernames for external users will be deactivated if unused for 28 months.

Usernames must not be shared.

3. Internal User - Usernames

A user must be identified to the network with a unique username assigned by the Department of Administration. Exceptions must be approved by the agency security officer and documented. All usernames that are not restricted, must have a password associated with them.

A username is to be deactivated when the individual user no longer needs access to a computer system or terminates employment with the agency. The agency security officer for the computer system or network must be notified by agency management to deactivate the username.

Usernames will be deactivated if unused for more than 90 days.

Usernames must not be shared.

4. External User – Passwords

Passwords will be at least six characters long and contain at least one numeric and one alphabetic character.

Passwords will be changed every six months or at the next login time if previous login time is greater than six months.

A password “hint” may be provided to users in the event that they lose or forget their current password.

The user password hint cannot be the same as the password or contained therein.

Passwords will not be reused for at least six cycles.

Passwords must not be written down where they can be found by unauthorized persons and must not be shared with other individuals.

5. Internal User - Passwords

Passwords will be at least six characters long and contain at least one numeric and one alphabetic character.

Initial passwords assigned to new usernames must be changed by the user at their initial login.

Passwords will be changed at least every 60 days.

Passwords will not be reused for at least six cycles.

Passwords must not be written down where they can be found by unauthorized personnel and must not be shared with other individuals.

When the computer system or network allows, users with administrative, root, supervisor, super user, etc. access must have passwords that are more complex. They should have a minimum of 8 characters using a combination of uppercase and lowercase letters, and numbers. Characters must not be consecutive within the password, like AAAAAAA1, they should be something more like Qn01Ppa3.

The warning level to users for forced password changes must be seven days or greater for systems with this capability.

The password cannot be the same as the username including the initial password.

6. Internal User - Access Rights

If a user changes work positions in an agency, their access rights must be reviewed and changed to match the new job position.

Agencies may restrict or extend computing privileges and access to their information resources (except in cases of specific federal or state statute.)

Access to network resources (programs, data, printers, etc.) is determined by the business process owner and/or authorized personnel and the rights or privilege are then assigned for each username.

Agencies may allow individuals, other than state employees and contractors, access to information for which the agencies are responsible, so long as such access does not violate any license or contractual agreement; state policy or any federal, state, county or local law or ordinance.

7. Implementation Timeframe

The modifications to this policy on June 2005 have implementation considerations. In addition to technical staff time, end user education will be necessary. Immediate compliance will be impossible for many agencies. The expectation is that agencies will start making implementation plans immediately, and compliance will be required by July 1, 2006.

C. Background - History On The Creation Of Or Changes To This Policy

This policy was originally called “UserID, Password & Access”, policy number S-GEN40, effective on January 17, 1997. It was modified in September 2000 to include requirements for SABHRS at the request of the Legislative Audit Division.

Based on recommendations from the Information Security Service Delivery Team, this policy was modified in October 2002 to include more specific requirements for passwords used by administrative UserIDs.

Recommendations for modifications of this policy were made by the enterprise Security Committee in January 2005 to meet Federal requirements, as well as to meet the needs for external usernames and passwords.

The January 2005 modifications were discussed at two ITMC meetings and at a separate ITSD sponsored meeting on May 10, 2005.

D. Guidelines - Recommendations, Not Requirements

It is recommended that every time a user is prompted to change their network password, that they change all of their application passwords, and other passwords at the same time.

Passwords should not be obvious or easily guessed (users' name, address, birth date, child's name, spouse's name, etc.)

It is recommended that agency personnel procedures specifically identify that an employee's IT authorizations be reviewed upon termination or change in job function.

User rights should be periodically reviewed.

E. Change Control and Exceptions

Policy changes or exceptions are governed by the Procedure for Establishing and Implementing Statewide Information Technology Policies and Standards. Requests for a review or change to this policy are made by submitting an Action Request form. Requests for exceptions are made by submitting an Exception Request form. Changes to policies and standards will be prioritized and acted upon based on impact and need.

III. Close

For questions or comments about this instrument, contact the Information Technology Services Division at ITSD Service Desk, or:

Chief Information Officer
PO Box 200113
Helena, MT 59620-0113
(406) 444-2700
FAX: (406) 444-2701

IV. Cross-Reference Guide

A. State/Federal Laws

- 2-17-505(1) – Policy
- 2-17-514(1) – Enforcement
- §2-17-505(2), MCA
- §2-17-512, MCA
- §2-15-114, MCA
- 2-17-512, MCA
- 2-17-534, MCA
- 2-15-114, MCA

B. State Policies (IT Policies, MOM Policies, ARM Policies)

- 2-15-112, MCA
- ARM 2.13.101 - 2.13.107 - Regulation of Communication Facilities
- MOM 3-0130 Discipline
- ARM 2.12.206 Establishing Policies, Standards, Procedures and Guidelines.

C. IT Procedures or Guidelines Supporting this Policy

- Policy: Establishing and Implementing Statewide Information Technology Policies and Standards
- Procedure: Establishing and Implementing Statewide Information Technology Policies and Standards

V. Administrative Use

Product ID:	ENT-SEC-063
Proponent:	Janet R. Kelly, Director, Department of Administration
Version:	1.1
Approved Date:	July 15, 2008
Effective Date:	June 2005
Change & Review Contact:	ITSD Service Desk
Review Criteria:	Event Review: Any event affecting this policy may initiate a review. Such events may include a change in statute, key staff changes or a request for review or change.
Scheduled Review Date:	July 1, 2013
Last Review/Revision:	Reviewed July 11, 2008. Non-material changes are necessary.
Change Record:	July 11, 2008 – Non-material changes made: - Standardize instrument format and common components. - Changed to reflect next review date.